

Zscaler

How to enable SSL scanning on your school's Zscaler web filter

How to enable SSL scanning on your schools Zscaler web filter:

Background Information:

If SSL scanning is not enabled the traffic that occurs using SSL cannot be attributed to a specific user and will show on your reports as the generic school traffic. Also the more granular controls cannot be applied and traffic can only be allowed or blocked.

How does SSL scanning work?

Zscaler SSL scanning works by configuring the Zscaler to be an intermediary of the secure transaction. Instead of having a single end to end secure transaction as is usual with https connections, the Zscaler terminates the connection from the website, inspecting the content of the packet for compliance with the web filtering policy and then Zscaler establishes a new SSL tunnel to the user's computer using the Zscaler certificate.

Legitimate SSL sites such as banking can be excluded from this Zscaler process and it is explained later in this document how to achieve this.

How to configure SSL Scanning for your School

-Installing the Zscaler digital certificate

- 1) You need to distribute the Zscaler SHA1 digital certificate to all devices on your network. For Windows networks this can be achieved very quickly using Group Policy. The SHA1 certificate can be obtained from the link below. The certificate should be installed in the "Trusted Root Certification Authorities" container.
- 2) If you are using iOS(Apple) based devices you will need to use whatever management software you have in place. If you do not have management software in place users can be instructed to go to the following URL to download the certificate for installation.

<http://www.ceomelb.catholic.edu.au/publications-policies/zscaler/>

-Configuring Zscaler to scan SSL (HTTPS) transaction

- 1) Login to the Zscaler Admin Portal

URL: <https://admin.zscalerone.net>

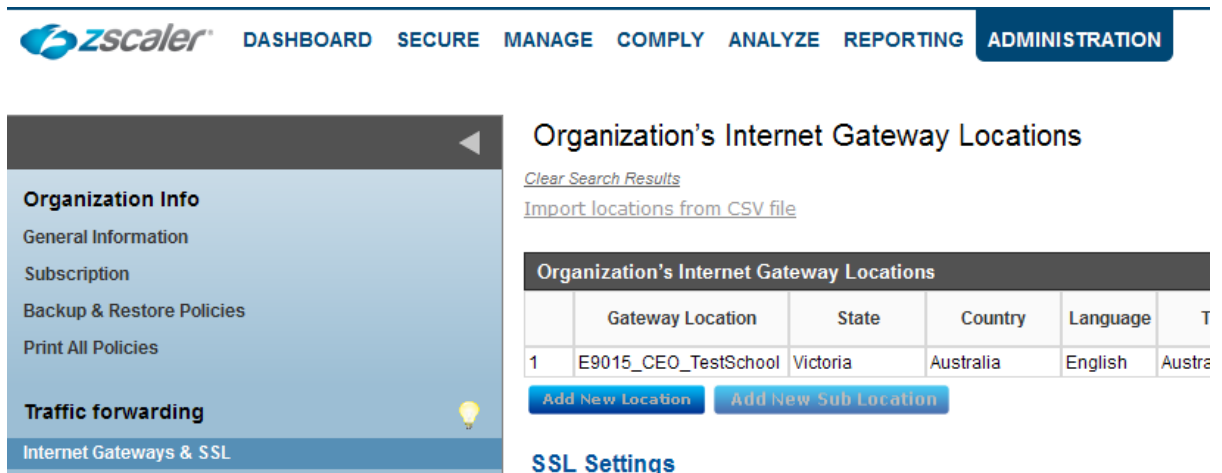
UN: siteadmin@your_School_Domain_name

PW: xxxx



The image shows the Zscaler Administration Interface login page. At the top, the Zscaler logo is on the left and "Administration Interface" is on the right. Below this, there are two input fields: "ZAdmin Login:" with the email "siteadmin@ceomelb.catholic.edu" and "Password:" with masked characters. A blue "Login" button is centered below the password field. At the bottom, a blue bar contains the copyright notice: "Copyright ©2007-2012, Zscaler, Inc. All rights reserved".

- 3) Browse to the "Administration" tab and then select "Internet Gateways & SSL" from the menu on the left.

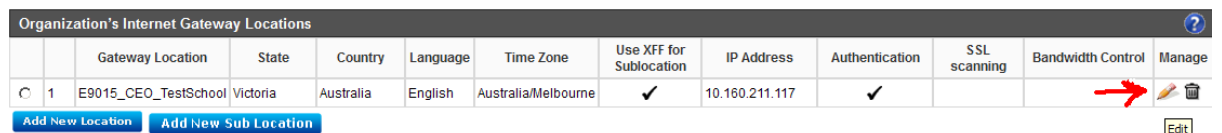


The image shows the Zscaler Administration Interface with the "ADMINISTRATION" tab selected. On the left, the "Internet Gateways & SSL" menu item is highlighted. The main content area is titled "Organization's Internet Gateway Locations". It includes links for "Clear Search Results" and "Import locations from CSV file". Below these is a table with the following data:



	Gateway Location	State	Country	Language	T
1	E9015_CEO_TestSchool	Victoria	Australia	English	Austr

Below the table are two buttons: "Add New Location" and "Add New Sub Location". Below the buttons is a link for "SSL Settings".

- 4) Once you are on this page select "Edit" and then select the pencil next to your sites gateway location as shown below;




The image shows the Zscaler Administration Interface with the "Organization's Internet Gateway Locations" table. The table has the following columns: Gateway Location, State, Country, Language, Time Zone, Use XFF for Sublocation, IP Address, Authentication, SSL scanning, Bandwidth Control, and Manage. The first row of data is highlighted, and a red arrow points to the "Manage" column, which contains a pencil icon and a trash icon. Below the table are two buttons: "Add New Location" and "Add New Sub Location".


	Gateway Location	State	Country	Language	Time Zone	Use XFF for Sublocation	IP Address	Authentication	SSL scanning	Bandwidth Control	Manage
1	E9015_CEO_TestSchool	Victoria	Australia	English	Australia/Melbourne	✓	10.160.211.117	✓			 

- 5) On the “Internet Gateway Location” configuration page, select the option to “Enable SSL Scanning” and then select “Done”.



Internet Gateway Location

Manage Internet Gateway Location	
Location	E9015_CEO_TestSchool
State	Victoria
Country	Australia
Language	English
Time Zone	Australia/Melbourne
XFF Forwarding	<input checked="" type="checkbox"/>
Static IP address(es)	10.160.211.117 Select
Authentication Required	<input checked="" type="checkbox"/>
Enable SSL Scanning (Allow the service to act as a proxy to decrypt and scan SSL encrypted traffic)	<input checked="" type="checkbox"/> 
Configure Bandwidth Available for this Location (Mbps)	
Enforce Bandwidth control for this location	<input type="checkbox"/>

- 6) This should then take you back to the main “Internet Gateway & SSL” configuration page. On this page change the “Notification style for blocked unscanned SSL transactions” to “Show notification page”. Then about two thirds of the way down the page is an option to enable SSL scanning based on the SHA1 algorithm. Make sure both settings are configured as shown below.

Organization's Internet Gateway Locations											
	Gateway Location	State	Country	Language	Time Zone	Use XFF for Sublocation	IP Address	Authentication	SSL scanning	Bandwidth Control	Manage
1	E9015_CEO_TestSchool	Victoria	Australia	English	Australia/Melbourne	<input checked="" type="checkbox"/>	10.160.211.117	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Add New Location		Add New Sub Location									

SSL Settings

SSL Configuration	
Block transactions which cannot be decrypted for technical reasons.	<input type="checkbox"/>
URL categories and custom domains for which SSL transactions will not be decrypted. Overrides per-location SSL scanning configuration.	Select
<small>Note: This exception list does not apply to Roadwarriors whose SSL traffic has been directed to port 9443 of the service.</small>	
Notification style for blocked unscanned SSL transactions	Show notification page 
URL categories and custom domains for which SSL transactions are blocked. Applied regardless of whether or not SSL interception is enabled.	Adult Material, Adult themes, Lingerie/Bikini, Nudity, Pornography, Sexuality, Adult Sex Education, K-12 Sex Education, Drugs, Gambling, Illegal or Questionable, Copyright Infringement, Computer Hacking, Questionable, Profanity, Mature Humor, Anonymizer, Image host, File host, Shareware download, Online chat, Militancy/Hate and Extremism, Alternate Lifestyle, Alcohol/Tobacco, Tasteless, Violence, Weapons/Bombs, Security, Spyware/Adware, Peer to Peer Site, Social Networking Adult Select
Untrusted Certificate Security Policy	When server certificate is signed by an untrusted issuer: <input checked="" type="radio"/> Pass through error message to browser <input type="radio"/> Deny transaction <input type="radio"/> Allow transaction with no user notification
<small>Note: If you enable SSL scanning, you must download the Cloud Service CA Certificate from this Link and ensure that all your users browsers have the Cloud Service CA Certificate installed as a trusted root CA. Caution: Depending on the local laws governing SSL inspection at your sites, enabling SSL inspection by the Zscaler proxy could have legal implications. Please ensure that turning on SSL inspection is in compliance with your corporate policy.</small>	
Use SSL Scanning Root CA Certificate Based on SHA1 Algorithm	<input checked="" type="checkbox"/> 

- 7) Now select “Save” in the top right hand corner of the web page. After you have selected “Save” you should be prompted for an option to “Activate Now”, select this.

- 8) The setting changes are now complete. Ensure that the page is showing all three changes correctly set as shown below;

Common troubleshooting and configuration changes post SSL Scanning implementation

- 1) Users are getting a certificate error when visiting a https web page .

- Ensure the user has the correct digital certificate installed on their device
- Ensure the certificate is installed in the “Trusted Root authorities” container on windows based devices.
- Verify that the site has a valid SSL certificate and the correct URL is used.

- 2) Why does traffic still show as the site ie “Exxxx_School_Name” in my reports?

- This is traffic that is generated from apps or browser widgets that do not use a cookie to access the internet. *For example the Facebook application installed on a iPad.*

- 3) Disable scanning on categories of sites that you trust and are of a personal nature ie Online Banking websites.

-Make the configuration changes shown below to the relevant categories.

SSL Settings

SSL Configuration	
Block transactions which cannot be decrypted for technical reasons.	<input type="checkbox"/>
URL categories and custom domains for which SSL transactions will not be decrypted. Overrides per-location SSL scanning configuration.	<div>Finance</div> <div>Select</div>
<small>Note: This exception list does not apply to Roadwarriors whose SSL traffic has been directed to port 9443 of the service.</small>	
Notification style for blocked unscanned SSL transactions	Show notification page
URL categories and custom domains for which SSL transactions are blocked. Applied regardless of whether or not SSL interception is enabled.	Adult Material, Adult themes, Lingerie/Bikini, Nudity, Pornography, Sexuality, Adult Sex Education, K-12 Sex Education, Drugs, Gambling, Illegal or Questionable, Copyright Infringement, Computer Hacking, Questionable, Profanity, Mature Humor, Anonymizer, Image host, File host, Shareware download, Online chat, Militancy/Hate and Extremism, Alternate Lifestyle, Alcohol/Tobacco, Tasteless, Violence, Weapons/Bombs, Security, Spyware/Adware, Peer to Peer Site, Social Networking Adult <div>Select</div>
Untrusted Certificate Security Policy	When server certificate is signed by an untrusted issuer: <input checked="" type="radio"/> Pass through error message to browser <input type="radio"/> Deny transaction <input type="radio"/> Allow transaction with no user notification
<small>Note: If you enable SSL scanning, you must download the Cloud Service CA Certificate from this Link and ensure that all your users browsers have the Cloud Service CA Certificate installed as a trusted root CA. Caution: Depending on the local laws governing SSL inspection at your sites, enabling SSL inspection by the Zscaler proxy could have legal implications. Please ensure that turning on SSL inspection is in compliance with your corporate policy.</small>	
Use SSL Scanning Root CA Certificate Based on SHA1 Algorithm	<input checked="" type="checkbox"/>

In this example we have made the finance category exempt from SSL scanning. This means when a user connects to their online banking website, this is a direct SSL connection between the users device and the banks server . Zscaler does not intercept/decrypt this traffic and consequently does not assign it to a user.